

Verfahren und Anordnung für den Schutz der Daten auf einer Smartcard

Patent number: DE19911673
Publication date: 2000-09-14
Inventor: KOEPPEN SIEGFRIED (DE)
Applicant: DEUTSCHE TELEKOM AG (DE)
Classification:
- **international:** G06F12/14; G06K19/073
- **european:** G06F21/00N1C6; G06F21/00N3J5D; G06K19/073;
G07F7/10D12
Application number: DE19991011673 19990309
Priority number(s): DE19991011673 19990309

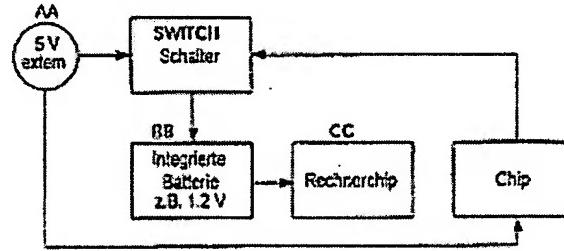
Also published as:

WO0054230 (A1)

[Report a data error here](#)

Abstract of DE19911673

Inferences to the processed data of the internal microchip can be effected on the contacts of the external power supply for a smart card by using appropriate measuring techniques - Differential Power Analysis (DPA). In order prevent misusage of smart cards, the DPA has to be effectively disabled. The invention permits a disabling of a DPA by decoupling the power supply voltage for the active computer chip from the external power supply for the smart card during calculation of confidential data. The technical solution can be attained by means of an integrated battery, a direct current stabilization, or by an integrated HF switched-mode power supply unit. When using direct current stabilization or an HF switched-mode power supply unit, the power supply voltage for the active computer chip can be conducted over a randomly controlled electronic switch so that the pulses still to be measured on the smart card contacts are additionally concealed.



AA ... 5V EXT.
BB ... INTEGRATED BATTERY e.g. 1.2 V
CC ... COMPUTER CHIP

Data supplied from the **esp@cenet** database - Worldwide

BEST AVAILABLE COPY

THIS PAGE BLANK (USPTO)

DE 199 11 673 A1 relates to a method for preventing an undesired so-called "attack", namely to prevent a so-called "differential power analysis" in order to determine internal processing steps carried out in an integrated smart card by analyzing the power fed to the smart card. For preventing such differential power analysis, the supply of energy to the chip is disconnected during the calculation. During the calculation of confidential data, the necessary power supply is provided by an internal battery. Alternatively, one can may use of a stabilized direct current supply or of an integrated high-frequency switching network. Therefore, this reference is neither concerned with asynchronous circuits nor does the reference teach to perform a time-variation of the supply voltage to an asynchronous circuit to thereby time-shift the execution time of operations within the asynchronous circuit.

47-10000-1000000000000000

THIS PAGE BLANK (USPTO)



(19) BUNDESREPUBLIK
DEUTSCHLAND

DEUTSCHES
PATENT- UND
MARKENAMT

(12) **Offenlegungsschrift**
(10) **DE 199 11 673 A 1**

(5) Int. Cl.⁷:
G 06 F 12/14
G 06 K 19/073

(21) Aktenzeichen: 199 11 673.3
(22) Anmeldetag: 9. 3. 1999
(43) Offenlegungstag: 14. 9. 2000

(11) Anmelder:
Deutsche Telekom AG, 53113 Bonn, DE

(12) Erfinder:
Köppen, Siegfried, Dipl.-Ing., 15711 Königs
Wusterhausen, DE

(56) Für die Beurteilung der Patentfähigkeit in Betracht
zu ziehende Druckschriften:
DE 195 06 921 C2

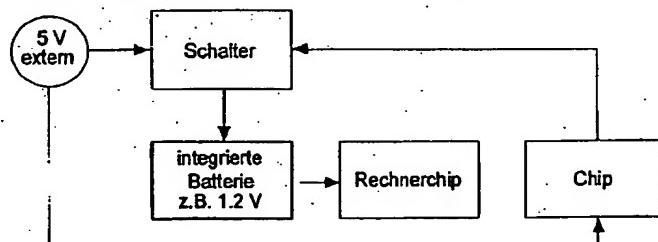
Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

(54) Verfahren und Anordnung für den Schutz der Daten auf einer Smartcard

(57) An den Kontakten der externen Stromversorgung für eine Smartcard sind mit geeigneter Meßtechnik Rückschlüsse auf die verarbeiteten Daten des internen Mikrochips möglich - Differential Power Analysis (DPA). Um einen Mißbrauch von Smartcards auszuschließen, muß die DPA wirkungsvoll verhindert werden.

Mit der vorliegenden Erfindung wird eine DPA dadurch verhindert, daß die Versorgungsspannung für den aktiven Rechnerchip während der Berechnung der vertraulichen Daten von der externen Stromversorgung für die Smartcard entkoppelt wird. Die technische Lösung kann durch eine integrierte Batterie, eine Gleichspannungsstabilisierung oder ein integriertes HF-Schaltnetzteil erreicht werden.

Bei Verwendung der Gleichspannungsstabilisierung oder eines HF-Schaltnetzteils kann die Versorgungsspannung für den aktiven Rechnerchip über einen zufallsgesteuerten elektronischen Schalter geführt werden, so daß zusätzlich eine Verschleierung der an den Smartcardkontakte noch zu messenden Impulse erreicht wird.



DE 199 11 673 A 1

Beschreibung

Die Erfindung betrifft das Gebiet des Schutzes der Daten auf einer Smartcard.

Nach dem Stand der Technik ist bekannt, daß an den Kontakten der Stromversorgung einer Smartcard mit Hilfe geeigneter Meßtechnik und Meßverfahren Rückschlüsse auf die verarbeiteten Daten des internen Mikrochips gezogen werden können. Besonders bei der Berechnung kryptografischer Algorithmen ist eine DPA "Differential Power Analysis" durch Hacker leicht möglich (siehe www.cryptography.com/dpa/technical/index.html – Autor Paul Kocher).

Mit der vorliegenden Erfindung soll erreicht werden, daß Rückwirkungen vom Rechnerchip an den äußeren Kontakten der Smartcard nicht auswertbar sind.

Die Aufgabe wird dadurch gelöst, daß Rückwirkungen vom Rechnerchip während der Berechnung der vertraulichen Daten durch stromversorgungsmäßige Entkoppelung von der externen Versorgungsspannung weitestgehend verhindert werden und zusätzlich eine Verschleierung noch auftretender Impulse angewendet werden kann.

Im einfachsten Fall wird die stromversorgungsmäßige Entkoppelung durch eine integrierte Batterie erreicht, die im Smartcard-Normalbetrieb über die externe Versorgungsspannung (z. B. 5 V) gepuffert wird und bei der Berechnung vertraulicher Daten den Rechnerchip galvanisch von der übrigen Schaltung abtrennt. Die Abtrennung der internen Batterie erfolgt softwaregesteuert über ein Mikrorelais oder einen elektronischen Schalter. Da die interne Batterie während der Berechnung der vertraulichen Daten von der externen Versorgungsspannung abgetrennt wird, ist eine DPA nicht möglich (siehe Fig. 1).

Es ist Stand der Technik, eine Batterie in eine Smartcard zu integrieren (siehe Wirtschaftswoche Nr. 4 vom 21.01.1999).

Anstelle der internen Batterie kann auch eine Gleichspannungsstabilisierung integriert werden, die durch Spannungs-umsetzung, z. B. von 5 V auf 1,2 V, den Rechnerchip von der übrigen Schaltung stromversorgungsmäßig entkoppelt (siehe Fig. 2). An den Eingangsklemmen der Stabilisierungsschaltung dürfen keine Rückwirkungen durch unterschiedliche Stromaufnahme (charakteristische Impulse) des Rechnerchips meßbar sein.

Optional kann die Stabilisierungsschaltung durch einen elektronischen Schalter gesteuert werden, um wahlweise oder zufallsgesteuert den Rechnerchip seine Versorgungsspannung zu liefern. In den Ausschaltlücken liefert ein integrierter Kondensator die Energie. Somit kann zusätzlich eine Verschleierung eventuell noch über die Klemmen der externen Stromversorgung (Smartcardkontakte) meßbarer Impulse erfolgen.

Eine stromversorgungsmäßige Entkoppelung für den Rechnerchip von der übrigen Schaltung kann auch durch ein hochfrequentes Schaltnetzteil erreicht werden, das anstelle der Batterie oder Gleichspannungsstabilisierung integriert wird (siehe Fig. 3). Die geschaltete Spannungswandlung kann z. B. von 5 V auf 1,2 V erfolgen. An den Eingangsklemmen des Schaltnetzeils dürfen keine Rückwirkungen durch unterschiedliche Stromaufnahme (charakteristische Impulse) des aktiven Rechnerchips meßbar sein.

Die geschaltete Spannungswandlung kann optional durch einen elektronischen Schalter gesteuert werden, um wahlweise oder zufallsgesteuert den Rechnerchip die Versorgungsspannung zu liefern. In den Ausschaltlücken liefert ein integrierter Kondensator die Energie. Somit kann eine Verschleierung eventuell doch noch über die externen Klemmen der externen Stromversorgung zu messenden Impulse erfolgen. Hier erfolgt eine doppelte Verschleierung,

denn der geschaltete Spannungswandler arbeitet vorzugsweise mit einer höheren Frequenz als die Taktfrequenz des Rechnerchips.

Patentansprüche

1. Verfahren für den Schutz der Daten auf einer Smartcard, dadurch gekennzeichnet, daß eine Auswertbarkeit der vom Rechnerchip berechneten vertraulichen Daten an den Kontakten für die externe Stromversorgung – Differential Power Analysis – dadurch verhindert wird, daß die Versorgungsspannung für den aktiven Rechnerchip während der Berechnung der vertraulichen Daten von der externen Stromversorgung entkoppelt wird, und daß zusätzlich eine Verschleierung der an den äußeren Smartcardkontakten noch auftretenden Impulse angewendet werden kann.
2. Anordnung für den Schutz der Daten auf einer Smartcard, dadurch gekennzeichnet, daß für die Entkopplung der Versorgungsspannung für den aktiven Rechnerchip von der externen Stromversorgung während der Berechnung der vertraulichen Daten durch folgende Bauteile erfolgen kann

- a) integrierte Batterie
- b) Gleichspannungsstabilisierung
- c) integriertes HF-Schaltnetzteil.

3. Anordnung nach Anspruch 2, dadurch gekennzeichnet, daß bei Verwendung von Gleichspannungsstabilisierung oder integriertem HF-Schaltnetzteil die Spannungszuführung zum aktiven Rechnerchip über einen zufallsgesteuerten elektronischen Schalter erfolgen kann und dadurch zusätzlich eine Verschleierung der an den äußeren Smartcardkontakten noch zu messenden Impulse erreicht wird.

Hierzu 1 Seite(n) Zeichnungen

- Leerseite -

BEST AVAILABLE COPY

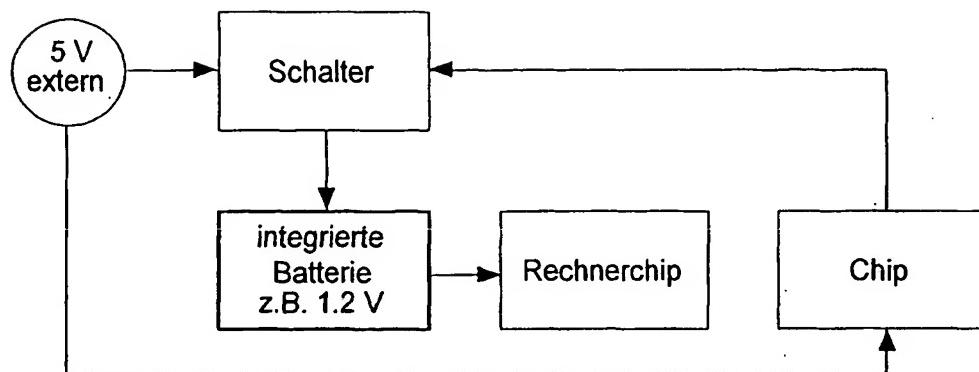


Fig. 1

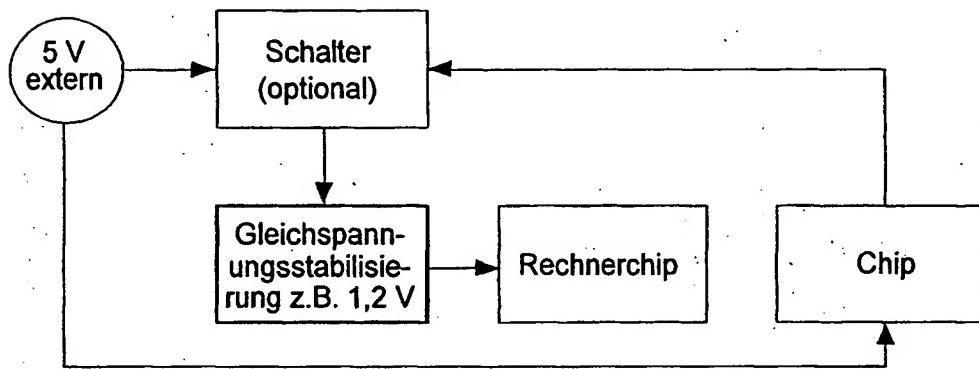


Fig. 2

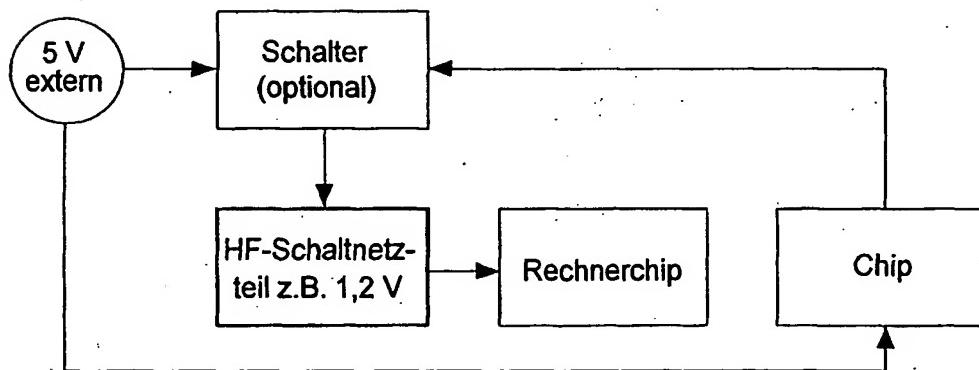


Fig. 3